Remarks

Claims 1, 3, 7-9, 13, 18, 23, 25, and 29 have been amended. Claims 17, 22, and 33 have been canceled. No claims have been added. Thus, claims 1-16, 18-21, and 23-32 are pending.

Allowable Subject Matter

Applicants acknowledge that claims 5-6, 11-12, 15-16, 20-21, 27-28, and 31-32 were objected to as being dependent upon rejected base claims, but would be allowable if rewritten in independent form. Applicants respectfully assert that the rejection of the independent claims from which they depend is overcome, meaning these claims are allowable as currently written.

Rejections under 35 U.S.C. § 102(e)

Claims 1-3, 7-9, 13, 18, 23-25 and 29 were rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,189,098 issued to Kaliski, Jr. (Kaliski). Applicants have amended independent claims 1, 7, 13, 18, 23, and 29 to overcome this rejection.

Claim 1 as amended recites the following:

> A method performed by a user terminal of a wireless access network, the method comprising:
>
> scrambling a user terminal certificate using a shared secret to be known only by the user terminal and an access point of the wireless access network, the scrambled user terminal certificate including a user terminal public key which corresponds to a user terminal private key;
>
> generating an authenticator string including data encrypted with the user terminal private key; and
>
> sending a message to the access point, **the message including the scrambled user terminal certificate and the authenticator string**.

Amended claims 7, 13, 18, 23, and 29 similarly contain the limitation of a message including the scrambled user terminal certificate and the authenticator string, wherein the scrambled user terminal certificate includes a user terminal public key and the authenticator string includes data encrypted with the user terminal private key. Claims 1, 7, and 23 recite a method, user terminal, and machine-readable medium for sending the message including the scrambled user terminal certificate and the authenticator string. Claims 13, 18, and 29 recite a method, access point, and machine-readable medium for receiving the message, unscrambling the user terminal certificate, and decrypting the authenticator string.

A user terminal certificate including a user terminal public key which corresponds to a user terminal private key finds support in canceled claims 17, 22, and 33. The element of an authenticator string including data encrypted with the user terminal private key finds support in the specification in paragraphs **[0025]-[0027]**, **[0037]-[0038]**, and **[0046]-[0049]**. No new matter has been added in amending the claims.

Kaliski discloses a method and system to authenticate a client without the use of a client public or private key. In Kaliski, the client certificate "need not include the public key of the client since authentication of the client by the server does not rely on the public key of the client." Col. 3, lines 55-58; see also col. 6, lines 24-25. No authenticator string is used because only the client and the server it trusts have access to the certificate; thus, the certificate itself is proof of the client's authenticity. See Col. 2, lines 34-36. Claims 1, 7, 13, 18, 23, and 29 recite the use of a certificate that includes a user terminal public key. The user terminal proves its authenticity by demonstrating, through the authenticator string, possession of the user terminal private key that corresponds to the user terminal public key. Therefore, Applicants respectfully submit that amended claims 1, 7, 13, 18, 23, and 29 contain limitations not disclosed by Kaliski. Applicants also submit that dependent claims 2, 3, 8, 9, 24, and 25, which necessarily include the limitations of the independent claims from which they depend, likewise contain limitations not disclosed by Kaliski.

Rejections under 35 U.S.C. § 103

Claims 4, 10, 26, 14, 19, and 30

Claims 4, 10, 26, 14, 19, and 30 were rejected under 35 U.S.C. 103(a) as being unpatentable over Kaliski in view of U.S. Patent No. 6,754,824 issued to Persson et al. (Persson). Applicants submit that, in light of the amendments to independent claims 1, 7, 13, 18, 23, and 29, claims 4, 10, 26, 14, 19, and 30 are not rendered obvious by Kaliski in view of Persson.

As discussed above, Kaliski does not disclose a message containing a scrambled user terminal certificate and an authenticator string, wherein the scrambled user terminal certificate includes a user terminal public key and the authenticator string includes data encrypted with a user terminal private key. These limitations are recited in independent claims 1, 7, 13, 18, 23, and 29.

The office Action at page 5 cites Persson as disclosing modifying the CRC code by initializing a linear feedback shift register (LFSR) by a common key known only to the participating nodes. Regardless of whether or not Persson discloses these limitations, Persson does not disclose a message containing a scrambled user terminal certificate and an authenticator string, wherein the scrambled user terminal certificate includes a user terminal public key and the authenticator string includes data encrypted with a user terminal private key. Thus, Persson fails to cure the deficiencies of Kaliski. Therefore, Applicants respectfully submit that independent claims 1, 7, 13, 18, 23, 29 are patentable over Kaliski and Persson. Applicants also submit that dependent claims 4, 10, 26, 14, 19, and 30 are also patentable over Kaliski and Persson because they contain at least the same limitations as the independent base claims they depend upon.

Claims 17, 22, and 33

Claims 17, 22, and 33 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Kaliski in view of U.S. Patent No. 6,886,095 issued to Hind et al. (Hind). Claims 17, 22, and 33 were canceled. However, a limitation from claims 17, 22, and 33 was added to independent claims 1, 7, 13, 18, 23, and 29. Specifically, the limitation that the user terminal certificate includes a user terminal private key which corresponds to a user terminal public key was added to independent claims 1, 7, 13, 18, 23, and 29.

The Office Action at page 6 cites Hind as disclosing a user terminal certificate including an identification of the user terminal and a user terminal public key which corresponds to a user terminal private key, wherein the user terminal certificate is used to authenticate the user terminal. Whether or not Hind discloses these limitations, Hind does not disclose a message containing a scrambled user terminal certificate and an authenticator string, wherein the scrambled user terminal certificate includes a user terminal public key and the authenticator string includes data encrypted with a user terminal private key. Thus, Hind fails to cure the deficiencies of Kaliski. Therefore, Applicants respectfully submit that amended independent claims 1, 7, 13, 18, 13, and 29 are patentable over Kaliski and Hind.

Conclusion

For at least the foregoing reasons, Applicants submit that the rejections have been overcome. Therefore, claims 1-16, 18-21, and 23-32 are in condition for allowance and such action is earnestly solicited. The Examiner is respectfully requested to contact the undersigned by telephone if such contact would further the examination of the above-referenced application.

Please charge any shortages and credit any overcharges to our Deposit Account number 02-2666.

Respectfully submitted,
BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN, LLP

Date: 7/21/06

Gregory D. Caldwell
Reg. No. 39,926

12400 Wilshire Boulevard
Seventh Floor
Los Angeles, CA 90025-1026
(408) 720-8598